March 25, 2016

John P. Holdren, PhD
Director
Office of Science and Technology Policy (OSTP)
Executive Office of the President

Dear Dr. Holdren,

On behalf of the Healthcare Information and Management Systems Society (HIMSS) and the Association of Medical Directors of Information Systems (AMDIS), we are pleased to provide written comments to the Office of the Science and Technology Policy (OSTP) in response to the Precision Medicine Initiative (PMI): Draft Data Security Policy Principles and Framework (PMI Principles and Framework). We appreciate the opportunity to leverage our members' expertise in commenting on the PMI Principles and Framework, and we look forward to continuing our dialogue with OSTP and other agencies on the Precision Medicine Initiative. We believe that the best possible policy principles and framework for data security comprise the necessary foundation for the Precision Medicine Initiative to be successful.

HIMSS is a global, cause-based, not-for-profit organization focused on better health through information technology (IT). In North America, HIMSS focuses on health IT thought leadership, education, market research, and media services. Founded in 1961, HIMSS North America encompasses more than 64,000 individuals, of which more than two-thirds work in healthcare provider, governmental, and not-for-profit organizations, plus over 640 corporations and 450 not-for-profit partner organizations, that share this cause.

Founded in 1997, AMDIS is the premier professional organization for physicians interested in and responsible for healthcare information technology. AMDIS Members are the thought leaders, decision makers and opinion influencers dedicated to advancing the field of Applied Medical Informatics and thereby improving the practice of medicine. With our symposia, blogs, on-line forum, journal, presentations, sponsored and co-sponsored programs, and networking opportunities, AMDIS truly is the home for the "connected" CMIO.

We applaud the application of the National Institute of Standards and Technology (NIST) Cybersecurity Framework (NISTCSF) to the PMI Principles and Framework. HIMSS has been involved with the development of the NISTCSF since its inception. HIMSS has provided comments to the three requests for information (RFIs) which NIST has furnished to date, including, most recently, a response to the December 2015 RFI.

Further, while many researchers have already been sharing PMI data by way of contractual agreements, the security standards, practices, and breach notification procedures, may vary from agreement to agreement. As a result, we support the use of the NISTCSF to help establish uniformity amongst PMI organizations with respect to use and disclosure of PMI data.

Our recommendations and comments focus on the following points:

- We recommend that the PMI Principles and Framework expand beyond research-based uses for PMI to include clinical application and uses of PMI.

- We recommend an expanded glossary in Appendix "A" of the PMI Principles and Framework so that terms of art are defined (e.g., PMI organization, PMI user, managers of PMI data, enclave approaches, genomic data, biospecimen-derived data, security elements, etc.).

- Jointly we recommend that the terms "de-identification" and "identifying information" should be defined in the expanded glossary in Appendix "A" of the PMI Principles and Framework. Many types of identifying information could be used to identify a participant, including gender and zip code, among others. The PMI Principles and Framework needs to fully address what the identifying information could be (i.e., identifiers of identifying information) so that entities and individuals are aware. Further, at least one rigorous and reliable process for de-identification of identifying information should be set forth in the PMI Principles and Framework.

- We recommend that the "full universe" of PMI users, managers, and handlers (and their organizations) needs to be defined. (To this end, a visual map of such PMI users, managers, and handlers may be helpful.) Once this is established, these individuals and entities can then apply the PMI Principles and Framework for appropriate and secure handling of PMI data.

- We recommend that the PMI Principles and Framework more fully address confidentiality, integrity, and availability of PMI data. Confidentiality, integrity, and availability of PMI data are mentioned in the document, but any true discussion of data security principles needs to include more in-depth treatment of these topics.

- We recommend that the PMI Principles and Framework provide additional guidance on physical security of PMI data, and the physical security of the facilities that house information systems, from which PMI data may be accessed or retrieved.

- Together we recommend that the PMI Principles and Framework should address which state and/or federal laws or regulations apply for the creation, receipt, transmission, and maintenance of PMI data. However, we does not advocate new laws or regulations for PMI data, or "novel" interpretations of such laws or regulations concerning PMI data.

- We recommend that PMI users should participate in mock phishing and other preparedness exercises-ideally, these exercises should address various threats and scenarios which may encompass the physical, administrative, and/or technical realms, as appropriate. These mock phishing and other preparedness exercises can help reinforce the training that PMI users receive. The exercises should be tailored to critical threats and/or frequent/most probable threats which may occur.

- We recommend guidance on what constitutes limiting exposure to PMI data.

- We strongly support the idea of sharing experiences and challenges so that organizations can learn from each other with respect to the precision medicine initiative, but there needs to be more guidance in terms of what exactly should be shared in terms of this part of the initiative.

As the PMI Data Security Policy Framework is based on the work of NIST, we are providing comments on key parts of the five NISTCSF Core Functions in the PMI Principles and Framework:

**Identify**

*Overall security plan.*
PMI data should be safeguarded wherever it may exist. We support the idea that PMI organizations need to know where the data is, who has it, who is doing what to it, and how it is being used, managed, or shared. With this in mind, the PMI data may reside or be accessible via mobile devices, in the cloud, websites, or through other means.

The overall security plan should be a written plan, regularly reviewed and updated. An integral part of the security plan is the risk assessment and management of those risks. A helpful guide is the HIMSS Risk Assessment Toolkit. In addition, the plan should be regularly tested and validated as well to ensure its appropriateness and accuracy. Personnel should be regularly trained on the plan.

In addition, security standards and best practices are evolving, including in the healthcare sector. Section 405 of the Cybersecurity Act of 2015, now codified at 6 U.S.C. §1533 (2016), calls for "a common set of voluntary, consensus-based, and industry-led guidelines, best practices, methodologies, procedures, and processes" for the healthcare sector. It would be advisable to regularly update this PMI Principles and Framework as such information evolves.

*Risk-based approach.*
We support the idea that PMI organizations need specific guidance on how to protect PMI data through the application of a risk-based approach. There should be different levels of protection for PMI data depending upon the type of the data, in addition to the form. The risk-based approach should address the lifecycle and flow of PMI data, internally within the organization, with patients, with other PMI organizations, and other external parties.

**Protect**

*Access Control-Identity Proofing.*
We request guidance on what level of assurance a PMI organization should have with respect to identity proofing of an individual and the "how to" in terms of the appropriate level of assurance. Additionally, both the sender and receiver of PMI data should be identity proofed (i.e., identity verification and validation).

*Access Control-Credentials; Authentication.*
PMI organizations should ensure that the credentials (even those used for multi-factor authentication) are not counterfeited or stolen. With this in mind, we recommend that the PMI Principles and Framework provide guidance in terms of what kinds of multi-authentication methods may be used to afford strong authentication.

In terms of risk-based authentication controls should not be easy to bypass or otherwise disable. The PMI Principles and Framework should provide guidance on recommended risk-based authentication controls.

*Access Control-Authorization.*
The PMI Principles and Framework states that PMI organizations should limit access, use, or disclosure based on what is necessary to satisfy a particular purpose or carry out a function. The PMI Principles and Framework further states that authorization controls should be granular enough to support participant consent that has been captured by the PMI organization. In this vein, PMI organizations should have a "PMI Notice of Privacy/Security Practices" (similar to how HIPAA requires a HIPAA Notice of Privacy Practices). To this end, we recommend that the PMI Principles and Framework include a PMI Notice of Privacy/Security Practices for PMI organizations to follow as a template.

**Detect**

*Audit Events.*
We ask for more specific guidance in the PMI Principles and Framework on which types of system and network events should be monitored (e.g., successful and unsuccessful attempted access to PMI data, potential insider threat activity indicators, etc.).

*Detection and Alerting.*
More guidance is also requested in terms of what kinds of anomalies, alerts, reported, and/or other relevant events should be made to the PMI organizations' governance boards. The information may be too voluminous, too technical, and too costly (both in terms of resources and manpower) to produce in report form.

**Respond**

*Incident Response.*
We support the idea that all PMI organizations should have a written incident response plan (which should include a communications plan, including who to communicate with, how, and when). Further, we recommend that the PMI Principles and Framework should be supplemented with additional guidance on what elements the incident response plan should contain. The written incident response plan should include tasks, such as identification of the incident, prioritization of the incident (e.g., is a quick response needed?), containment of the incident, eradication of the incident, and mitigation of the incident. The plan should also address who comprises the computer security incident response team and what roles they play. Finally, a the PMI Principles and Framework should emphasize an appropriate number of personnel who should be trained on the plan.

*Incident Response Testing*.
The PMI Principles and Framework should emphasize organization-based testing of the incident response plan, to include organizations conducting mock exercises to assess the effectiveness of the plans, training, and any gaps or deficiencies which may exist.

*Affected Individual Notification.*
We recommend additional guidance in the PMI Principles and Framework on which breach notification laws and/or regulations may apply at the state and federal levels if PMI data were breached. In addition, what constitutes a "breach" of PMI data should also be included in the future guidance.

*Accountable Point of Contact.*
We recommend that the PMI Principles and Framework provide more information on a written communications plan that will work in concert with the PMI organization's incident response plan. PMI organizations should have a written communications plan to coordinate the activities and initiatives relevant to the incident response function, including individuals' roles, coordination of individuals, incident commander, etc. PMI organizations should also identify more than one accountable point of contact for coordinating with appropriate organizations and affected individuals at the appropriate times. A single point of contact may lead to a single point of failure.

**Recover**

*Incident and Breach Recovery Plan.*
We recommend that the PMI Principles and Framework provide additional guidance on the recovery phase. The goal of the recovery phase is for the organization to resume normal operations as quickly as possible. The recovery plan should address what people, processes, and technology are necessary to do this. The recovery plan should address the restoration of PMI data (and associated applications and systems) in a quick and efficient manner to minimize disruptions to the organization (and the services which it delivers, including delivery of care and coordination of care). People, processes, and technology all need to be addressed in the recovery plan—all need to be aligned in order for the recovery to be as quick and efficient as possible.

*Lessons Learned.*
We recommend that the PMI Principles and Framework provide additional guidance on resilience. PMI organizations would benefit from becoming more resilient based upon lessons learned, consistent with the Executive Order No. 13636 on "Improving Critical Infrastructure Cybersecurity" and Presidential Policy Directive No. 21 on "Critical Infrastructure and Resilience." The lessons learned should extend to people, processes, and technology (including the careful coordination of all three of these elements). With this in mind, gap analysis should be done with an eye towards all three of these elements and any identified gaps should be addressed by the PMI organization. Further, once the lessons learned have been formulated in view of a security incident, this information should be reported to the governance board, at an appropriate

level of detail. Using these steps, PMI organizations can become more resilient against future security incidents and less vulnerable to attack and compromise.

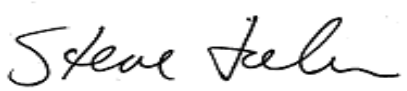
We are committed to being a resource to OSTP on the Precision Medicine Initiative to help with its mission to enable a new era of medicine through research, technology, and policies that empower patients, researchers, and providers to work together toward development of individualized care.

We look forward to the opportunity to further discuss these issues with you in more depth. Please feel free to contact Jeff Coughlin, Senior Director of Federal & State Affairs, at 703.562.8824, or Eli Fleet, Director of Federal Affairs, at 703.562.8834, with questions or for more information.

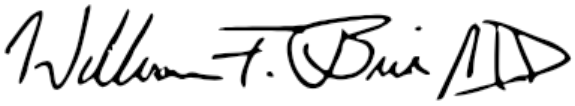
Thank you for your consideration.

Sincerely,

Dana Alexander RN, MSN, MBA, FAAN, FHIMSS
Vice President, Clinical Advisory
Divurgent
Chair, HIMSS North America Board of Directors



H. Stephen Lieber, CAE
President & CEO
HIMSS



William F. Bria, MD,
Board Chairman
AMDIS

Richard L. Rydell, MBA
CEO
AMDIS

Howard Landa, MD
Board Vice-Chairman
AMDIS